

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

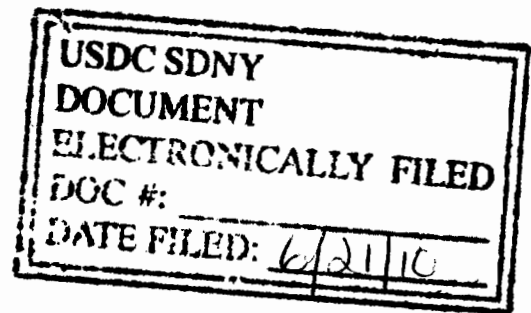
PASSLOGIX, INC.,

Plaintiff,

- against -

2FA TECHNOLOGY, LLC, 2FA, INC.,
GREGORY SALYARDS, and SHAUN
CUTTILL,

Defendants.



OPINION AND ORDER

08 Civ. 10986 (PKL)

APPEARANCES

PROSKAUER ROSE LLP
Steven M. Kayman, Esq.
Dan Goldberger, Esq.
1585 Broadway
New York, N.Y. 10036-8299

CADWALADER, WICKERSHAM & TAFT LLP
Hal S. Shaftel, Esq.
One World Financial Center
New York, N.Y. 10281

Attorneys for Plaintiff

LAURENCE SINGER, ATTORNEY-AT-LAW
Laurence Singer, Esq.
1629 K Street NW, Suite 300
Washington, D.C. 20006

Attorney for Defendants

LEISURE, District Judge:

Currently before the Court is defendant 2FA Technology, LLC's and 2FA, Inc.'s (collectively, "2FA") motion, pursuant to Federal Rule of Civil Procedure ("Rule") 65, for a preliminary injunction. 2FA asks the Court to enjoin Passlogix, Inc. ("Passlogix") from marketing, distributing, and selling the software products v-GO AM and v-GO UAM, which, according to 2FA, contain 2FA trade secrets that have been misappropriated by Passlogix. For the reasons set forth below, 2FA's motion for a preliminary injunction is DENIED.

BACKGROUND

The Court assumes familiarity with the facts and procedural history of this case. See Passlogix, Inc. v. 2FA Tech., LLC, 08 Civ. 10986, 2010 U.S. Dist. LEXIS 43473 (S.D.N.Y. May 4, 2010) (Leisure, J.); Passlogix, Inc. v. 2FA Tech., LLC, 08 Civ. 10986, 2010 U.S. Dist. LEXIS 44182 (S.D.N.Y. Apr. 27, 2010) (Leisure, J.). Accordingly, the Court only discusses those facts that are necessary to the resolution of the instant motion.¹

¹ 2FA's motion originally was briefed in September 2009. The resolution of 2FA's motion was postponed so that this Court could address allegations that 2FA had committed a fraud on the Court. See Passlogix, 2010 U.S. Dist. LEXIS 44182. The parties were permitted to supplement their original briefing with additional arguments, which this Court has considered in full.

I. The Parties and Their Relationship

Passlogix and 2FA are in the business of developing and selling security-related software for managing access to restricted computerized systems. See Passlogix, 2010 U.S. Dist. LEXIS 44182, at *3. The software at issue in this motion is Passlogix's v-GO Access Accelerator Suite ("v-GO"), a set of products "designed to simplify and streamline sign-on to computer systems and reduce the number of passwords managed by end-users." (2FA's Mem. in Supp. of Mot. for a Prelim. Inj. ("2FA Mem.") 4.) Among other functions, "v-GO encrypts and stores user passwords so users do not have to remember them." (Passlogix's Mem. in Opp'n to Mot. for a Prelim. Inj. ("Passlogix Mem.") 3.) 2FA contends that two of Passlogix's v-GO software programs, v-GO AM and v-GO UAM, contain trade secrets that Passlogix misappropriated from 2FA.

In early 2006, Passlogix and 2FA began to collaborate on the development of a credential management system ("CMS"), "a product to administer the creation, utilization, replacement and expiration of ID cards or 'smart cards' used for access to computers and physical entry to buildings." (Id.) On April 24, 2006, the parties signed a License Agreement, whereby 2FA granted Passlogix, subject to certain restrictions, "a non-exclusive, perpetual license to modify, adapt, enhance, improve, support, maintain, translate and create derivative works of

[certain 2FA software] in both Source Code and Object Code form." (See Sept. 2, 2009, Decl. of Marc Boroditsky ("Boroditsky Sept. Decl.") Ex. 1 at 3.) The License Agreement was modified on four separate occasions between March 2007 and October 2008.

2FA agrees that it granted Passlogix "the rights to include [2FA's] licensed [s]oftware . . . into its v-GO [software suite], and to promote and market the resulting package as v-GO CMS, later changed to v-GO CM, under the Passlogix name," as well as "rights to possess 2FA['s] [] object and source code." (2FA Mem. 6.) In return, Passlogix was to pay 2FA defined royalty payments, milestone payments, and "Customization Fees." (See Passlogix Mem. 4-5.) Passlogix and 2FA disagree, however, as to the scope of the License Agreement and its subsequent amendments.

The relationship between Passlogix and 2FA began to deteriorate almost immediately after the License Agreement was signed. (See 2FA Mem. 9; Passlogix Mem. 5-8.) Passlogix contends that 2FA misrepresented its technical capabilities, and, from the onset of its relationship with Passlogix, that 2FA "consistently supplied versions of 2FA CMS that did not meet contractual specifications." (Passlogix Mem. 6.) Passlogix claims that "due to deficiencies with 2FA's deliverables, Passlogix was unable to timely launch [its new v-GO product] and

repeatedly was forced to defer marketing and/or delivery." (Id. at 7.) Passlogix further contends that, due to 2FA's severe financial problems, 2FA marketed its CMS technology to a company other than Passlogix in violation of the portions of the License Agreement that granted Passlogix the exclusive right to "use, sublicense, [] market, promote, demonstrate and distribute" 2FA's software. (Id. at 9.)

While admitting that the relationship between Passlogix and 2FA became "frayed almost immediately after the License Agreement was executed," 2FA contends that it met all of its obligations under the License Agreement. (2FA Mem. 9-10.) 2FA alleges that Passlogix repeatedly modified its expectations for the work 2FA was expected to perform pursuant to the License Agreement, and that 2FA spent "over 1000 man hours" responding to Passlogix's changing demands. (Id. at 9.)

II. The Purported Trade Secrets

Based solely on 2FA's submissions in support of its motion for a preliminary injunction, it is unclear what purported trade secrets 2FA claims Passlogix has misappropriated. 2FA repeatedly refers to its source code as a trade secret, but also references software functionalities, as well as undefined "other intellectual property," as trade secrets that have been misappropriated by Passlogix. (See 2FA Mem. 19 ("2FA's source

code and other intellectual property is all over Passlogix's computers"); 2FA's Reply Mem. in Supp. of Mot. for a Prelim. Inj. ("2FA Rep. Mem.") 9 (stating that "Passlogix is clearly still in possession of 2FA's intellectual property, including its source code"); May 2, 2010, Declaration of Shaun Cuttill ("Cuttill May Decl.") ¶ 1 (identifying 2FA's PKCS#11 mapping technology "as one of [2FA's] many trade secrets").)

At oral argument, counsel for 2FA clarified that, for purposes of the present motion for a preliminary injunction, the only trade secret 2FA is claiming has been misappropriated by Passlogix is 2FA's technology concerning PKCS#11 mapping. (See Transcript of May 5, 2010, Hearing ("Tr.") 6:16-9:23.) However, even this limited purported trade secret is not defined easily.

PKCS#11 is a computer protocol that "enable[s] different software programs to communicate with each other for the purposes of encrypting and decrypting data often times stored on smart cards." (Sept. 2, 2009, Decl. of Mark Manza ("Manza Sept. Decl.") ¶ 16.) 2FA describes its trade secret relating to PKCS#11 mapping as "a unique methodology for determining how best to interact with a given smart card." (Cuttill May Decl. ¶ 1.) Broadly stated, 2FA alleges that it invented a distinctive methodology for mapping different cryptographic service providers ("CSPs") to an appropriate PKCS#11 library, thereby enabling multiple computer applications to interact with

multiple types of smart cards. (See id. ¶¶ 1-2.) 2FA claims that its particular method of enabling communications between a smart card and middleware² "is the only approach that maps a CSP to a PKCS[#]11 library" (id. ¶ 4), and that 2FA's approach facilitates the "use of multiple different (and often incompatible) implementations . . . [such as the use of] multiple smart cards from multiple vendors." (April 12, 2010, Decl. of Shaun Cuttill ("Cuttill Apr. Decl.") ¶ 4.) Due to its unique PKCS#11 mapping technology, 2FA claims its software is able "to work with over 100 different smart cards on the market that employ a mix of various types of technology standards." (2FA Rep. Mem. 8.)

2FA admits that standards for PKCS#11 are publicly available. (See 2FA Rep. Mem. 7.) However, Shaun Cuttill, 2FA's Chief Technology Officer and the individual who designed over 90% of 2FA's PKCS#11 mapping technology, claims that the specific trade secret at issue is not limited to the publicly available standards for PKCS#11, and that the source code employed by 2FA does not contain publicly available source code. (Cuttill Apr. Decl. ¶ 4) In making these assertions, 2FA distinguishes the publicly available general standards for PKCS#11 from the specific manner by which these standards are

² "Middleware is a manufacturer-specific application that works with that manufacturer's smart cards [in order to recognize] a specific card." Cuttill May Decl. ¶ 2.

implemented and supported by 2FA. (See 2FA Rep. Mem. 7.) 2FA claims that its ability "to seamlessly support many different . . . means of implementing [PKCS#11] standards" is the trade secret that Passlogix has misappropriated. (Id. 8.)

III. The Technology at Issue

A. Background

Passlogix's v-GO Access Accelerator Suite consists of at least seven software products. (See Manza Sept. Decl. ¶ 2.) The two v-GO products that are the subject of 2FA's preliminary injunction motion are v-GO AM and v-GO UAM. Taken as a whole, the v-GO products "function together to provide comprehensive security functionality," including so-called "strong authentication" capabilities. (Id. ¶¶ 2, 4.) Strong authentication refers to the verification of an individual's identity through the use of two or more unique means; such as the use of a smart card and a typed password, or a smart card and a fingerprint scan. (See April 28, 2010, Decl. of Marc Boroditsky ("Boroditsky Apr. Decl.") ¶ 7.) The purpose of strong authentication technology is to make it more difficult for unauthorized users to access a computer system. "For example, if an authorized user loses his or her card, an unauthorized person who finds it would still need a [password] to gain access to the computer system." (Id. ¶ 10.)

Both v-GO AM and v-GO UAM offer strong authentication capabilities, and require the operator of a computer to use a combination of a smart card or proximity card and a typed password to gain access to a computer system. (Id. ¶ 11.) Passlogix has been offering strong authentication in its v-GO AM product since December 2004, (see Manza Sept. Decl. ¶ 4), while v-GO UAM was released initially on March 31, 2010. (See 2FA's Suppl. Mem. of Law in Supp. of its Mot. for Prel. Inj. ("2FA Suppl. Mem.") 4.) The main difference between v-GO AM and v-GO UAM is that v-GO AM connects a user to Passlogix's Single Sign On ("SSO") software,³ while v-GO UAM allows a user to connect to Passlogix's SSO as well as to Microsoft Windows. (See Boroditsky April Decl. ¶ 13.)

B. Design and Development of PKCS#11 Capabilities

In early 2007, Passlogix began testing whether v-GO CM—the product developed, subject to the License Agreement, in conjunction with 2FA—was compatible with v-GO AM. (See Manza Sept. Decl. ¶ 15.) During the period of testing it became clear that v-GO CM was not compatible with v-GO AM. (See id.) The lack of compatibility between the two products was due to the

³ When using SSO technology a user inputs his or her password at the time they log on to Windows. The SSO software then automatically retrieves the correct username and password for each application that the user opens while he or she is signed on to Windows. (See Boroditsky April Decl. ¶ 4.)

fact that, at the time, v-GO AM did not support PKCS#11 libraries,⁴ while v-GO CM, which included 2FA's technology, supported PKCS#11 libraries. (See id. ¶ 16; Passlogix Rep. Mem. 5-6.)

Passlogix and 2FA agree that, after the failed period of testing, Passlogix redesigned v-GO AM and launched a new version of the product that contained support for PKCS#11 libraries. (See Manza Sept. Decl. ¶ 19; 2FA Rep. Mem. 6-7.) Passlogix and 2FA disagree, however, as to how this additional functionality was added to v-GO AM, and similarly, how this functionality came to be included in v-GO UAM. It is this disagreement that forms the crux of the present dispute.

Passlogix contends that its employees created and implemented the modifications that allowed v-GO AM to support PKCS#11 libraries without the use of any source code from 2FA. (See, e.g., Passlogix Mem. in Supp. of Summ. J. and in Further Opp'n. to 2FA's Mot. for Prel. Inj. ("Passlogix Fur. Mem.") 15.) Passlogix supports this position with declarations submitted by Mark Manza, the company's Chief Technology Officer, who states that after discovering the lack of compatibility between v-GO CM and v-GO AM—namely that v-GO CM used PKCS libraries while v-GO AM used a different set of standards known

⁴In early 2007 v-GO AM supported a protocol known as MSCAPI, which Passlogix describes as "similar, but distinct" from PKCS#11. (Manza Decl. ¶ 16.)

as MSCAPI—"Passlogix elected to build PKCS#11 support . . . into [v-GO] AM, rather than requiring 2FA to further delay its efforts by asking [2FA] to add the required support for [MSCAPI] to its software." (April 28, 2010, Decl. of Marc Manza ("Manza Apr. Decl.") ¶ 11.)

Manza claims that 2FA was made aware of the compatibility problems between v-GO CM and v-GO AM and that Cuttill, 2FA's Chief Technology Officer, offered to "send over code that would help bridge the compatibility gap." (Id. ¶ 12.) According to Manza, he and Stephan Wardell, a senior software engineer at Passlogix, reviewed the 2FA code supplied by Cuttill but ultimately rejected the idea of using 2FA's source code in v-GO AM, and instead chose to build the PKCS#11 support structure themselves. (See id. ¶ 16.) Manza claims that after rejecting the possibility of using code supplied by 2FA, "Wardell . . . assumed principal responsibility for adding PKCS#11 support to v-GO AM" and that "Passlogix built its PKCS#11 support using Passlogix's existing architecture for interfacing with third-party software—entirely different from (and commercially superior to) 2FA's methods." (Id.) Manza claims that 2FA was advised of the changes being made to v-GO AM and that Cuttill was "glad to see" that PKCS#11 support was being added to v-GO AM. (Id. ¶ 17.)

2FA, in contrast, presents a more nefarious narrative behind the development of the PKCS#11 support capabilities in v-GO AM and v-GO UAM. 2FA argues that by 2007, Passlogix recognized that it "desperately required . . . PKCS#11 support for the marketing and sales of its products" and that it added this function to v-GO AM by misappropriating 2FA's source code. (2FA Suppl. Mem. 2.) 2FA claims that while Passlogix recognized "a growing market for strong authentication products," Passlogix "had little or no strong authentication expertise" of its own. (2FA Mem. 29.) Faced with this challenge, 2FA claims that Passlogix entered into the License Agreement, which gave Passlogix access to 2FA's trade secrets, and then developed "strong authentication functionalities and products on its own through the use of 2FA's trade secrets." (2FA Mem. 29.) 2FA claims that in 2007, Passlogix copied 2FA's trade secrets concerning PKCS#11 technology directly into v-GO AM "and used the trade secrets to expand its knowledge and know-how of strong authentication" and to develop products that "are competitive with 2FA's offerings." (2FA Mem. 20-21.) 2FA claims that the "same PKCS#11 intellectual property" that Passlogix copied in to v-GO AM now has been "shared and incorporated into [v-GO] UAM" as well. (2FA Suppl. Mem. 3.)

In addition to using 2FA's PKCS#11 technology in v-GO AM and v-GO UAM, 2FA contends that Passlogix has failed to protect

2FA's source code properly. (See 2FA Mem. 16; 2FA Suppl. Mem. 9.) 2FA argues that its "trade secrets and proprietary information . . . [have] been freely distributed to personnel not authorized to have access to such information" and that, in the course of discovery in this case, Passlogix improperly has produced documents containing 2FA's source code. (2FA Mem. 16.) While 2FA claims that its source code is "is all over Passlogix's computers" and has been shared with Passlogix employees who do not have a need to view the source code, 2FA does not allege that 2FA's source code has been disseminated to any third parties. (See Tr. 32:1-4 (counsel to 2FA clarifying that 2FA is "not alleging that there's been dissemination [of 2FA's purported trade secrets] to third parties . . .").

IV. Evidence of Misappropriation

Rather than relying on expert testimony or a direct comparison between 2FA's source code and the code used in Passlogix's products, 2FA supports its claim that Passlogix has misappropriated 2FA's purported trade secrets by relying on statements made by Passlogix employees in e-mail messages, and by declarations submitted by Cuttill, who is a defendant in this case.

A. E-mails and Other Written Communication

2FA claims that internal Passlogix e-mail messages demonstrate, among other things, that "Passlogix had little to no strong authentication experience or expertise before signing the License Agreement" with 2FA (2FA Mem. 7); that "Passlogix possessed a strong desire to end [its] relationship with 2FA but not before gaining control of 2FA's trade secrets" (id. 11); that Passlogix considered offering to purchase 2FA's source code for a fraction of what it was worth (see id.); and that "Passlogix engineers [have] openly admit[ted] that only after reviewing, analyzing, and learning from 2FA['s] [] source code were they able to add missing functionalities" to v-GO AM and v-GO UAM (id. 14). 2FA focuses much of its attention on one e-mail chain in particular: messages sent between Manza and Wardell in April 2007 (the "April E-mail Chain"). 2FA views these messages as "a crucial piece of evidence" (Tr. 50:6-7) that provides proof of misappropriation that is so strong as to alleviate any need for expert testimony. (Tr. 26:1-5.)

The April E-mail Chain is between Manza, Passlogix's Chief Technology Officer, and Wardell, the individual at Passlogix who wrote the PKCS#11 source code for v-GO AM. (See April 28, 2010, Declaration of Daniel Goldberger, Esq., ("Goldberger Apr. Decl."), Ex. 15; Passlogix Fur. Mem. 15.) Manza begins the April E-mail Chain by stating that he "would like to review PKCS#11 authentication capability" for Passlogix's products and

that Cuttill "indicated that he has code that can support any PKCS library . . . so we would not be limited and could support any smartcard." (Goldberger Apr. Decl. Ex. 15 at 4.) Manza concludes by asking Wardell to speak with Cuttill about this issue. (Id.)

After speaking with Cuttill, Wardell provides Manza a summary of the conversation, which is followed by a series of back-and-forth e-mail communications between the two Passlogix employees. (See id. at 1-3.) Wardell begins by writing that he "spoke with [Cuttill] today about the PKCS#11 code" and that "it sounds promising." (Id. at 2.) Wardell indicates that he has not yet seen the PKCS#11 source code in question, but that he has been able to identify a number of tasks that Passlogix would need to perform if it wished to implement 2FA's PKCS#11 technology. These tasks include "add[ing] support for the PKCS#11 operations [Passlogix] need[s] that aren't already" in 2FA's code, creating "an interface to wrap this code," and converting the code from the computer language used by 2FA to the language used by Passlogix. (Id.) In addressing the issue of converting 2FA's source code to a format that could be used by Passlogix, Manza writes that he is "not sure if [Passlogix] can even use [2FA's] . . . code since we do not own it. I want to be sure we implement something that we own. So if we need to recreate it for our own purposes, that may be where we need to

go." (Id. at 3.) Wardell responds that he believes "it would take only 3-4 days" to rewrite 2FA's source code into the programming language used by Passlogix, but that there is a lot of additional work that would need to be done if Passlogix were to use 2FA's source code. (See id.) Manza then replies that "it seems [Passlogix does not] need anything from 2FA but the mapping data and beyond that we would build the rest ourselves." (Id.)

The next day, on April 26, 2007, Wardell continued the correspondence with Manza by writing that he had "spent some time reviewing" the 2FA code and decided that, "[a]s it stands right now, there is very little to work with. The basic mechanisms are in place, but there is little in terms of actual implementation." (Id. at 1.) Wardell notes that the 2FA source code lacks "CSP support" and "that the mappings between smartcards and PKCS#11 libraries is hardcoded, which means that as we add support for additional cards, the code would have to be updated and re-released." (Id.) Manza responds by asking if "it is safe to say that we [Passlogix] can build this ourselves, make it externally configurable so new cards don't mean rebuilding code" and that "other than the hardcoded definitions that help find the PKCS libraries, we could build the rest of the support ourselves without 2FA involvement?" (Id. at 1-2.) Wardell replies in the affirmative, stating that, "[y]es we can

definitely build this ourselves" and that "there is no need for 2FA involvement [] moving forward with this." (Id. at 2.)

2FA and Passlogix disagree as to the relevance of the April E-mail Chain. 2FA argues that the April E-mail Chain is strong evidence of Passlogix's misappropriation, as it demonstrates that Passlogix looked at 2FA's PKCS#11 source code, that Passlogix studied the methodology of the code, and that Passlogix used 2FA's source code in its products, while at the same time "looking for ways to keep 2FA's source code and cut [2FA] out" of the development of new products. (Tr. 56:4-20.) Passlogix, in contrast, argues that the April E-mail Chain supports its position that "[Passlogix] looked at [2FA's] code, [Passlogix] didn't like it much, and [Passlogix] decided to go it on our own" and design the PKCS#11 support independent from 2FA. (Tr. 14:9-14.)

B. Cuttill's Opinions

There is no independent expert opinion supporting 2FA's claims of misappropriation. Instead of relying on an expert, 2FA submits numerous declarations from Cuttill in support of its claim that Passlogix has misappropriated 2FA's trade secrets.⁵

⁵ 2FA also submits a declaration from Greg Salyards, 2FA's President and CEO. However, Salyards declaration largely focuses on the business relationship between 2FA and Passlogix, and does not address in great depth the alleged misappropriation of 2FA's intellectual property.

In his declarations, Cuttill asserts that he "personally authored over 90% of" 2FA's products, (Cuttill April Decl. ¶ 4), and that, much in the same way that "a designer or architect of a car or a bicycle could most certainly identify [his] unique implementations from those created by his peers," (id. ¶ 10), he is able to "state conclusively that the intellectual property" used by Passlogix "is the same intellectual property created by [him] and owned by 2FA." (Id. ¶ 11.)

In addition to these opinions, which Cuttill formed after reviewing "a Passlogix product licensed to Oracle" (see id. ¶ 6),⁶ Cuttill's opinion that Passlogix has misappropriated 2FA's PKCS#11 technology is based on a review of Passlogix e-mails, log files detailing when Passlogix employees accessed source code, a review of a presentation that demonstrated the capabilities of v-GO UAM, and Cuttill's own personal experience in software security. (See id. ¶ 14; Cuttill Jul. Decl. ¶ 8; Cuttill May Decl. ¶ 7.) Cuttill's opinion that Passlogix has misappropriated 2FA's trade secrets also is based on the argument that, prior to the sharing of information with

⁶ In his April declaration, Cuttill claims that Passlogix has provided 2FA's trade secrets to Oracle Corporation—presumably through an agreement that permits Oracle to re-brand and sell Passlogix software. (Cuttill April Decl. ¶ 14.) However, at oral argument held in May of this year, counsel for 2FA clarified that 2FA was not asserting that any of its purported trade secrets have been disseminated by Passlogix to third parties. (See Tr. 32:1-4 ("[2FA is] not alleging that there's been dissemination [of trade secrets] to third parties other than the parties within Passlogix who have had access to the source code that don't have authority to have access to the source code."))

Passlogix pursuant to the parties' License Agreement, 2FA was the only company in the computer security industry to employ PKCS#11 mapping technology. (See Cuttill May Decl. ¶¶ 2-5.) Because Passlogix added PKCS#11 mapping technology to v-GO AM, and eventually to v-GO UAM, after viewing 2FA's source code, Cuttill appears to argue that that the misappropriation of 2FA's trade secrets can be presumed.

DISCUSSION

The Court first addresses the standard for a preliminary injunction. Next, the Court addresses 2FA's claim that it will suffer irreparable harm if a preliminary injunction is not granted. Because the issue of irreparable harm is dispositive, the Court does not address whether 2FA has demonstrated that it likely will succeed on the merits of this case.

I. Preliminary Injunction Standard

"A preliminary injunction is 'an extraordinary and drastic remedy,'" Int'l Creative Mgmt., Inc. v. Abate, No. 07 Civ. 1979, 2007 U.S. Dist. LEXIS 22964, at *6 (S.D.N.Y. Mar. 28, 2007) (Leisure, J.) (quoting Med. Soc'y of State of N.Y. v. Toia, 560 F.2d 535, 538 (2d Cir. 1977)), and is "'one of the most drastic tools in the arsenal of judicial remedies.'" Id. (quoting Hanson Trust PLC v. SCM Corp., 774 F.2d 47, 60 (2d Cir. 1985)). To

obtain a preliminary injunction, a party must show: "(1) that [it] will be irreparably harmed if an injunction is not granted, and (2) either (a) a likelihood of success on the merits or (b) sufficiently serious questions going to the merits to make them a fair ground for litigation, and a balance of the hardships tipping decidedly in its favor." Lusk v. Vill. of Cold Spring, 475 F.3d 480, 485 (2d Cir. 2007) (quoting Bronx Household of Faith v. Bd. of Educ., 331 F.3d 342, 348-49 (2d Cir. 2003) (internal quotation marks omitted)); see also County of Nassau, N.Y. v. Leavitt, 524 F.3d 408, 414 (2d Cir. 2008).

"The threat of irreparable injury is a sine qua non" of a preliminary injunction: "If there is no irreparable injury, there can be no preliminary injunction." Am. Airlines, Inc. v. Imhof, 620 F. Supp. 2d 574, 579 (S.D.N.Y. 2009) (Kaplan, J.) (citations omitted); see also Faiveley Transp. Malmo AB v. Wabtec Corp., 559 F.3d 110, 118 (2d Cir. 2009) ("A showing of irreparable harm is 'the single most important prerequisite for the issuance of a preliminary injunction.'" (quoting Rodriguez v. DeBuono, 175 F.3d 227, 234 (2d Cir. 1999))). "[T]o satisfy the irreparable harm requirement, [the moving party] must demonstrate that absent a preliminary injunction [it] will suffer an injury that is neither remote nor speculative, but actual and imminent, and one that cannot be remedied if a court waits until the end of trial to resolve the harm." Faiveley,

559 F.3d at 118 (quoting Grand River Enter. Six Nations, Ltd. v. Pryor, 481 F.3d 60, 66 (2d Cir. 2007) (internal quotation marks omitted)).

"A district court should generally consider delay in assessing irreparable harm," since a delay in seeking a preliminary injunction undercuts the movant's claim of irreparable harm. Tom Doherty Assocs., Inc. v. Saban Entm't, Inc., 60 F.3d 27, 38 (2d Cir. 1995) (citation omitted); see also Citibank, N.A. v. Citytrust, 756 F.2d 273, 276 (2d Cir. 1985) (stating that delay may indicate "an absence of the kind of irreparable harm required to support a preliminary injunction" (citing Gillette Co. v. Ed Pinaud, Inc., 178 F. Supp. 618, 622 (S.D.N.Y. 1959))).

II. Irreparable Harm

2FA has not demonstrated that it will suffer irreparable harm if a preliminary injunction is not issued.

Both 2FA and Passlogix rely on the Second Circuit's decision in Faiveley to support their respective arguments concerning irreparable harm. (See Tr. 31:12-14 (Counsel to 2FA stating that, "[t]he Faiveley case is certainly the case on point here and the controlling case"); Passlogix Mem. 16 (relying on Faiveley for the proposition that a preliminary injunction is inappropriate "where the technology in dispute is

part of a defined product sold by a litigant and is not being generally disseminated to third parties").) Faiveley concerns the alleged misappropriation of trade secrets involving brakes used on subway cars. See Faiveley, 559 F.3d at 113. The plaintiff in Faiveley moved for a preliminary injunction to, among other things, prevent the defendant from entering into new contracts to manufacture, supply, or sell the subway brake components at issue. See id. at 115. The district court granted the application for a preliminary injunction. See id. Upon finding "an absence of evidentiary support of irreparable harm," the Second Circuit reversed the judgment of the district court, holding that the lower court abused its discretion in granting the preliminary injunction. Id. at 120.

The Circuit Court in Faiveley began its discussion of the irreparable harm standard by stating that it is incorrect to conclude that "a presumption of irreparable harm automatically arises upon the determination that a trade secret has been misappropriated." Id. at 118. The Court clarified that:

A rebuttable presumption of irreparable harm might be warranted in cases where there is a danger that, unless enjoined, a misappropriator of trade secrets will disseminate those secrets to a wider audience or otherwise irreparably impair the value of those secrets. Where a misappropriator seeks only to use those secrets—without further dissemination or irreparable impairment of value—in pursuit of profit, no such presumption is warranted because an award of damages will often provide a complete remedy for such an injury. Indeed, once a trade secret is

misappropriated, the misappropriator will often have the same incentive as the originator to maintain the confidentiality of the secret in order it profit from the proprietary knowledge.

Id. at 119-20. With this clarification in mind, the Circuit Court addressed the issue that, while defendant had used plaintiff's proprietary information for over twelve years, plaintiff "has not alleged that [defendant] unlawfully disseminated any trade secrets associated with the [products at issue] during that period, nor did the District Court find that [defendant] disclosed the trade secrets to any third party" and furthermore, there was evidence that, because defendant had "incurred considerable expense in developing" the product that the plaintiff claimed contained the misappropriated trade secrets, "[d]isclosure of [plaintiff's] trade secrets . . . would only undermine the competitive advantage [the defendant] has sought." Id. at 119. The Circuit Court then recounted the district court's findings that defendant "is not disseminating [plaintiff's secrets] or other know-how to any third parties; indeed, [defendant] appears to be treating them with the same confidentiality that they give to their own proprietary information *[T]here is no reason to conclude that [plaintiff's] trade secrets will be 'lost forever' absent injunctive relief.*" Id. (quoting Faiveley Transp. Malmo AB v. Wabtec Corp., 572 F. Supp. 2d 400, 409 (S.D.N.Y. 2008))

(emphasis original). The Circuit Court went on to conclude that, "[i]n light of [plaintiff's] failure to demonstrate . . . that [plaintiff] would suffer irreparable harm unless [defendant] was enjoined from disseminating its trade secrets, the District Court was without authority" to grant a preliminary injunction. Id.

In this case, 2FA alleges that certain non-essential employees within Passlogix have access to 2FA's source code, but 2FA has made clear that it is not alleging that Passlogix has disseminated 2FA's alleged trade secrets to third parties. (See Tr. 32:1-4 ("We [2FA] are not alleging that there's been dissemination [of the purported trade secrets] to third parties other than parties within Passlogix who have had access to the source code that don't have authority to have access to the source code.")) 2FA argues that this admission is not fatal to its claim of irreparable harm because, unlike the defendant in Faiveley, Passlogix does not protect 2FA's trade secrets with the same degree of care that it uses to protect its own proprietary information. (See 2FA Rep. Mem. 11 ("It is not only dissemination to third parties who have no right of access to the trade secrets It is also failing to treat trade secrets . . . with the same confidentiality that they [Passlogix] give to their own proprietary information."); Tr. 32:17-20 ("[I]t is very difficult for Passlogix to argue that

they're treating 2FA's trade secrets with the same confidentiality that they give their own proprietary information.") This argument lacks both factual and legal merit.

As an initial matter, 2FA has not demonstrated that Passlogix protects 2FA's purported trade secrets in a less-careful manner than it protects its own trade secrets. In support of its argument, 2FA contends that Passlogix has allowed 2FA's source code to "linger in emails and on its computer systems" (2FA Rep. Mem. 11); that 2FA's source code "is all over Passlogix's computers" (2FA Mem. 19); and that Passlogix "provided thousands of pages of 2FA's source code" during the course of discovery. (Tr. 32:15-16.) Passlogix refutes these arguments by noting that, to the extent any portions of 2FA's source code either still exist on Passlogix's computers or have been produced in discovery, the source code is in the body of e-mails that both parties agreed should not be destroyed. (See Passlogix Mem. 21; Manza Sept. Decl. ¶¶ 22-25.) Passlogix further maintains that "the only persons at Passlogix who received emails containing portions of 2FA's source code were members of the Passlogix v-GO CM team," and that, to the extent that non-technical personnel at Passlogix received e-mails containing 2FA source code, these e-mails came from 2FA, not Passlogix. (Passlogix Mem. 21; see also Tr. 68:20-25.) 2FA,

therefore, has not demonstrated that Passlogix fails to afford 2FA's purported trade secrets the same degree of protection it affords its own trade secrets.

More importantly, 2FA's argument suffers from a flawed understanding of irreparable harm. 2FA has not shown how it would suffer irreparable harm if, despite not being disseminated to third parties, Passlogix were to maintain 2FA's source code in a less secure manner than it maintains its own source code. Whether Passlogix treats 2FA's source code with less care than it treats its own source code may be a relevant factor in assessing whether 2FA's source code has been, or possibly will be, disseminated to third parties. This, however, is an argument that 2FA chose not to make (see Tr. 31:23-32:4), and 2FA provides no reason to conclude that Passlogix's confidentiality practices likely will cause 2FA's purported trade secrets to be "lost forever," or otherwise irreparably harmed. See Faiveley, 559 F.3d at 118. In other words, 2FA is incorrect that the manner by which Passlogix maintains 2FA's trade secrets—solely in comparison to the manner it maintains its own trade secrets, and removed from any consideration of possible disclosure to third parties—is an independent "second criteria" that satisfies the irreparable harm requirement.

Even if the Court were to interpret 2FA's contentions to include the argument that Passlogix's alleged comparatively

careless approach to the maintenance of 2FA's source code likely is to result in the dissemination of this code to third parties, 2FA's argument still would fail. As discussed above, the Court is not convinced that Passlogix has failed to protect 2FA's source code adequately. Furthermore, if, as 2FA alleges, the success of v-GO AM and v-GO UAM is based on Passlogix's incorporation of 2FA's trade secrets, it is in Passlogix's own self-interest to ensure that these trade secrets are protected. 2FA has provided no reason for this Court to believe that Passlogix is likely to undermine its own business opportunities by disclosing 2FA's source code to third parties. See, e.g., Synergy Advanced Pharms., Inc. v. Capebio, LLC, No. 10 Civ. 1736, 2010 U.S. Dist. LEXIS 53252, at *17-18 (S.D.N.Y. June 1, 2010) ("To demonstrate irreparable harm, a plaintiff must show an imminent danger that a defendant is likely to disseminate the protected information—an eventuality that should not be presumed given that the 'misappropriator will often have the same incentive as the originator to maintain the confidentiality of the secret in order to profit from the proprietary knowledge.'" (quoting Faiveley, 559 F.3d at 118-19)).

The Court concludes that 2FA has not shown that it will suffer an irreparable injury if a preliminary injunction is not granted. To the extent that 2FA is concerned that, absent a preliminary injunction, it would be "'in business' with a

company it does not trust" (2FA Mem. 21), 2FA does not show how any losses from such a venture could not be quantified in monetary terms.⁷ See Twentieth Century Fox Film Corp. v. Marvel Entm'ts, 277 F.3d 253, 260 (2d Cir. 2002) (Newman, J.) (preliminary injunction properly denied where any harm suffered by the moving party is quantifiable); The Proctor & Gamble Co. v. Ultreo, Inc., 574 F. Supp. 2d 339, 353 (S.D.N.Y. 2008) (finding no irreparable harm where moving party claimed "lost sales—which are easily quantifiable at trial and can be remedied with money damages"); Iron Mt. Info. Mgmt. v. Taddeo, 455 F. Supp. 2d 124, 132 (E.D.N.Y. 2006) (Bianco, J.) ("A preliminary injunction is not appropriate where monetary damages will serve as adequate compensation."). Furthermore, 2FA's cursory statements—devoid of supporting evidence concerning affected product lines, lost business relationships, and why such losses cannot be quantified in monetary terms—that it will lose goodwill and market share if a preliminary injunction is not granted, do not support a finding that 2FA is in imminent danger of suffering irreparable harm. See Pontone v. York Group, Inc., No. 08 Civ. 6314, 2008 U.S. Dist. LEXIS 80372, at *7-8 (S.D.N.Y. Oct. 10, 2008) ("Although . . . a loss of prospective goodwill

⁷ As there is an independent basis to conclude that 2FA has not demonstrated irreparable harm, the Court need not consider the argument that 2FA's delay in bringing its preliminary injunction motion demonstrates a lack of irreparable harm.

can constitute irreparable harm, . . . there must be a clear showing that a product that a plaintiff has not yet marketed is a truly unique opportunity for a company." (quoting Tom Doherty Assocs., 60 F.3d at 38)); Doldo Bros. v. Coors Brewing Co., No. 08 Civ. 206, 2008 U.S. Dist. LEXIS 17646, at *19-20 (N.D.N.Y. Mar. 7, 2008) ("Although the loss of good will can, in certain circumstances, equate with irreparable harm, simply invoking the phrase is insufficient to make the critical finding to support a preliminary injunction."); Park W. Radiology v. CareCore Nat'l LLC, 240 F.R.D. 109, 113 (S.D.N.Y. 2007) (denying preliminary injunction where movant did not show that its services were "so unique that any alleged damages resulting from its inability to market and sell them could not be easily quantified."); Jay's Custom Stringing v. Jonghwan Yu, No. 01 Civ. 1690, 2001 U.S. Dist. LEXIS 9298, at *23 (S.D.N.Y. July 26, 2001) ("If irreparable harm is remote, speculative, or a mere possibility, the motion must be denied."); c.f. O.D.F. Optronics Ltd. v. Remington Arms Co., No. 08 Civ. 4746, 2008 U.S. Dist. LEXIS 74482, at *18-19 (S.D.N.Y. Sept. 26, 2008) (citations omitted) ("The cases involving irreparable harm from a loss of goodwill or business relationships typically involve a situation in which a dispute between parties leads to the inability of one party to provide its product or products to the market or its customers. . . . The Second Circuit has reversed a finding of irreparable

harm where the facts demonstrate no loss of goodwill, but only provable monetary damages from the loss of a profitable line of business.").

Having concluded that 2FA cannot "meet its burden of demonstrating 'a likelihood of irreparable harm if the requested relief is denied,' the Court need not consider the likelihood of success on the merits or the balance of equities." Ultreo, Inc., 574 F. Supp. 2d at 356 (quoting Time Warner Cable, Inc. v. DIRECTV, Inc., 497 F.3d 144, 152-53 (2d Cir. 2007)); see also Pryor, 481 F.3d at 68 ("The finding of no showing of irreparable harm is dispositive.").

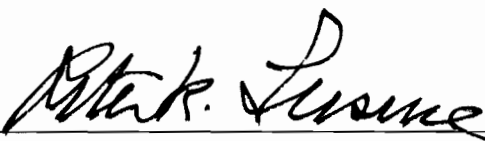
CONCLUSION

For the reasons stated above, 2FA's motion for a preliminary injunction is DENIED.

SO ORDERED.

New York, New York

June 21, 2010

A handwritten signature in black ink, appearing to read "Peter K. Lurie", is written over a horizontal line.

U.S.D.J.